IN THE CLAIMS:

Claims 1-50 are currently pending in this application.

Claims 3-5, 7-9, 15, 16, 19-21, 23-25, 29, 32, 35-37, 39-40, 47 and 48 are original;

Claims 1, 2, 6, 10-14, 17, 22, 26-28, 30, 31, 33, 34, 38, 41-46, 49 and 50 are previously amended;

Claim 18 is presently amended.

Please amend the claims as follows:

1. (Previously amended) A method for generating identification data, comprising the steps of:

providing an ATM PIN related to a first transaction type which is an ATM transaction; and

performing a cryptographic operation upon the ATM PIN, thereby generating a non-ATM electronic commerce PIN for use in a second transaction which is a non-ATM transaction.

2. (Previously amended) A method according to claim 1, wherein the step of performing a cryptographic operation comprises:

providing a conversion key; and

using the conversion key to perform said cryptographic operation upon the ATM PIN.

3. (Original) A method according to claim 2, wherein the step of providing a conversion key comprises:

providing conversion key derivation data;

providing a conversion key derivation key; and

performing a cryptographic operation upon the conversion key derivation data and the conversion key derivation key.

4. (Original) A method according to claim 3, wherein the step of performing a cryptographic operation upon the conversion key derivation data and the conversion key derivation key comprises using the conversion key derivation key to perform at least one cryptographic operation upon the conversion key derivation data.

5. (Original) A method according to claim 4, wherein the conversion key derivation data includes an identification number that is associated with multiple accounts, and wherein at least one cryptographic operation using a secret key is performed to cryptographically process said conversion key derivation data to produce the conversion key.

6. (Previously amended) A method according to claim 1, wherein the step of performing a cryptographic operation comprises:

providing cryptographically-computed data; and

performing an operation upon the ATM PIN and the cryptographically-computed data.

7. (Original) A method according to claim 6, wherein the step of providing cryptographically- computed data comprises:

providing initial data; and

performing at least one cryptographic operation using a secret key upon the initial data, thereby producing the cryptographically-computed data.

8. (Original) A method according to claim 7, wherein said at least one cryptographic operation using a secret key comprises at least one of a DES-encryption and a DES-decryption.

9. (Original) A method according to claim 8, wherein at least a portion of the initial data is obtained from at least a portion of an account number.

10. (Previously amended) A method according to claim 9, wherein the operation upon the ATM PIN and the cryptographically-computed data comprises either a subtraction operation or an addition operation.

11. (Previously amended) A method according to claim 10, wherein the step of providing cryptographically-computed data further comprises generating a cryptographically-computed number having a base corresponding to a base of a number representing the ATM PIN, wherein said cryptographically-computed number has a number of digits corresponding to a number of digits of said number representing the ATM PIN.

12. (Previously amended) A method according to claim 6, wherein the step of providing cryptographically-computed data comprises generating a cryptographically-computed number having a base corresponding to a base of a number representing the ATM PIN, wherein said cryptographically-computed number has a number of digits corresponding to a number of digits of said number representing the ATM PIN.

13. (Previously amended) A method according to claim 6, wherein the operation upon the [first set of identification data] ATM PIN and the

cryptographically-computed data comprises either a subtraction operation or an addition operation.

14. (Previously amended) A method for generating a cryptography key which corresponds to a bank or issuer identification number, comprising:

providing a key derivation key;

using the key derivation key in a cryptographic operation performed on data obtained from an identification number, thereby producing the cryptographic key.

15. (Original) A method according to claim 14, further comprising generating a key-check value suitable for determining whether data received corresponds to the cryptography key.

C1

16. (Original) A method according to claim 15, wherein the step of generating a key-check value comprises:

using a portion of the cryptography key to DES-encrypt a system-wide constant, thereby producing a first key-check value generation result;

using a portion of the cryptography key to DES-decrypt the first key-check value generation result, thereby producing a second key-check value generation result;

using a portion of the cryptography key to DES-encrypt the second key-check value generation result, thereby producing a third key-check value generation result; and

selecting a portion of the third key-check value generation result for use as a key-check value.

17. (Previously amended) A system for generating identification data, comprising:

a memory for storing an ATM PIN; and

a processor for performing a cryptographic operation upon the ATM PIN, such that said processor generates a second non-ATM PIN related to a non-ATM electronic transaction.

18. (Currently amended) The system of claim 17, wherein the memory includes means for storing a conversion key, and wherein the processor comprises means for using the conversion key to perform a cryptographic operation upon the ATM PIN.

19. (Original) The system of claim 18, wherein the memory further includes:

means for storing conversion key derivation data; and

means for storing a conversion key derivation key; and

wherein the processor comprises means to perform a cryptographic operation upon the conversion key derivation data and the conversion key derivation key, thereby generating the conversion key.

20. (Original) The system of claim 19, wherein the cryptographic operation upon the conversion key derivation data and the conversion key derivation key comprises at least one DES operation.

21. (Original) The system of claim 20, wherein the conversion key derivation data is derived from an identification number, and wherein said at least one DES operation comprises:

using a portion of the conversion key derivation key to DES-encrypt the conversion key derivation data, thereby producing a first conversion key generation result;

using a portion of the conversion key derivation key to DES-decrypt the first conversion key generation result, thereby producing a second conversion key generation result;

using a portion of the conversion key derivation key to DES-encrypt the second conversion key generation result, thereby producing a third conversion key generation result;

using the third conversion key generation result as a first portion of the conversion key;

using a portion of the conversion key derivation key to DES-encrypt the third conversion key generation result, thereby producing a fourth conversion key generation result;

using a portion of the conversion key derivation key to DES-decrypt the fourth conversion key generation result, thereby producing a fifth conversion key generation result;

C1

using a portion of the conversion key derivation key to DES-encrypt the fifth conversion key generation result, thereby producing a sixth conversion key generation result; and

using the sixth conversion key generation result as a second portion of the conversion key.

22. (Previously amended) The system of claim 17, wherein the memory includes means for storing cryptographically-computed data, and wherein the processor comprises:

means for generating the cryptographically-computed data; and

means for performing an operation upon the ATM PIN and the cryptographically-computed data.

23. (Original) The system of claim 22, wherein the memory further includes means for storing initial data, and wherein the means for generating the

cryptographically-computed data comprises means for performing at least one cryptographic operation upon the initial data, thereby producing the cryptographically-computed data.

24. (Original) The system of claim 23, wherein said at least one cryptographic operation comprises at least one of a DES-encryption and a DES-decryption.

25. (Original) The system of claim 24, wherein the initial data is obtained from an account number, wherein the memory further includes means for storing a conversion key, and wherein the cryptographic operation uses the initial data and the conversion key to produce the cryptographically-computed data.

26. (Previously amended) The system of claim 25, wherein the means for performing an operation upon the ATM PIN and the cryptographically-computed data comprises either a subtraction means or an addition means.

27. (Previously amended) The system of claim 25, wherein the means for performing an operation further comprises means for generating a cryptographically-computed number having a base corresponding to a base of a number representing the ATM PIN, wherein said cryptographically-computed number has a number of digits corresponding to a number of digits of said number representing the ATM PIN.

28. (Previously amended) The system of claim 22, wherein the means for performing an operation comprises means for generating a cryptographically-computed number having a base corresponding to a base of a number representing ATM PIN,

wherein said cryptographically-computed number has a number of digits corresponding to a number of digits of said number representing the ATM PIN.

29. (Original) The system of claim 22, wherein the means for performing an operation comprises either a subtraction means or an addition means.

30. (Previously amended) A system for generating a cryptography key which corresponds to a bank or issuer identification number, comprising:

a memory, comprising

means for storing a key derivation key; and

means for using the key derivation key in a cryptographic operation performed on data obtained from an identification number, thereby producing the cryptographic key.

C1

31. (Previously amended) The system of claim 30, further comprising:

a processor, wherein the processor further comprises means for generating a key-check value suitable for determining whether the data corresponds to the cryptographic key; and

a means for receiving data.

32. (Original) The system of claim 31, wherein the means for generating a key-check value comprises:

means for storing a system-wide constant;

means for using a portion of the cryptography key to DES-encrypt the system-wide constant, thereby producing a first key-check value generation result;

means for using a portion of the cryptography key to DES-decrypt the first key-check value generation result, thereby producing a second key-check value generation result;

means for using a portion of the cryptography key to DES-encrypt the second key-check value generation result, thereby producing a third key-check value generation result; and

means for selecting a portion of the third key-check value generation result for use as a key-check value.

33. (Previously amended) A system for generating identification data, comprising:

a memory;

a processor in communication with the memory; and

a computer-readable medium in communication with the processor and storing instructions which, when executed, cause the processor to perform the steps of:

storing an ATM PIN in the memory, said first set being related to a first transaction type; and

performing a cryptographic operation upon the ATM PIN, thereby generating a second PIN related to a non-ATM electronic transaction.

34. (Previously amended) The system of claim 33, wherein the step of performing a cryptographic operation comprises:

providing a conversion key;

storing the conversion key in the memory; and

using the conversion key to perform said cryptographic operation upon the ATM PIN.

35. (Original) The system of claim 34, wherein the step of providing a conversion key comprises:

storing conversion key derivation data in the memory;

storing a conversion key derivation key in the memory; and

performing a cryptographic operation upon the conversion key derivation data and the conversion key derivation key.

36. (Original) The system of claim 35, wherein the step of performing a cryptographic operation upon the conversion key derivation data and the conversion key derivation key comprises using the conversion key derivation key to perform at least one DES operation upon the conversion key derivation data.

37. (Original) The system of claim 36, wherein the conversion key derivation data is derived from an identification number, and wherein said at least one DES operation comprises:

using a portion of the conversion key derivation key to DES-encrypt the conversion key derivation data, thereby producing a first conversion key generation result;

using a portion of the conversion key derivation key to DES-decrypt the first conversion key generation result, thereby producing a second conversion key generation result;

using a portion of the conversion key derivation key to DES-encrypt the second conversion key generation result, thereby producing a third conversion key generation result;

using the third conversion key generation result as a first portion of the conversion key;

using a portion of the conversion key derivation key to DES-encrypt the third conversion key generation result, thereby producing a fourth conversion key generation result;

using a portion of the conversion key derivation key to DES-decrypt the fourth conversion key generation result, thereby producing a fifth conversion key generation result;

using a portion of the conversion key derivation key to DES-encrypt the fifth conversion key generation result, thereby producing a sixth conversion key generation result; and

using the sixth conversion key generation result as a second portion of the conversion key.

38. (Previously amended) The system of claim 33, wherein the step of performing a cryptographic operation comprises:

providing cryptographically-computed data;

storing the cryptographically-computed data in the memory; and

performing an operation upon the ATM PIN and the cryptographically-computed data.

39. (Original) The system of claim 38, wherein the step of providing cryptographically-computed data comprises:

storing initial data in the memory; and

performing at least one cryptographic operation using a secret key upon the initial data, thereby producing the cryptographically-computed data.

40. (Original) The system of claim 39, wherein said at least one cryptographic operation using a secret key comprises at least one of a DES-encryption and a DES-decryption.

41. (Previously amended) The system of claim 40, wherein at least a portion of the initial data is obtained from at least a portion of an account number.

42. (Previously amended) The system of claim 41, wherein the operation upon the ATM PIN and the cryptographically-computed data comprises either a subtraction operation or an addition operation.

43. (Previously amended) The system of claim 42, wherein the step of providing cryptographically-computed data further comprises generating a cryptographically-computed number having a base corresponding to a base of a number representing the ATM PIN, wherein said cryptographically-computed number has a number of digits corresponding to a number of digits of said number representing the ATM PIN.

C1

44. (Previously amended) The system of claim 38, wherein the step of providing cryptographically-computed data comprises generating a cryptographically-computed number having a base corresponding to a base of a number representing the ATM PIN, wherein said cryptographically-computed number has a number of digits corresponding to a number of digits of said number representing ATM PIN.

45. (Previously amended) The system of claim 38, wherein the operation upon the ATM PIN and the cryptographically-computed data comprises either a subtraction operation or an addition operation.

46. (Previously amended) A system for generating a cryptography key which corresponds to a bank or issuer identification number, comprising:

a memory;

a processor in communication with the memory; and

a computer-readable medium in communication with the processor and storing instructions which, when executed, cause the processor to perform the steps of:

storing a key derivation key in the memory;

using the key derivation key in a cryptographic operation performed on data obtained from an identification number, thereby producing the cryptographic key.

47. (Original) The system of claim 46, wherein the instructions, when executed, further cause the processor to perform the step of generating a key-check value suitable for determining whether data received corresponds to the cryptography key.

48. (Original) The system of claim 47, wherein the step of generating a key-check value comprises:

storing a system-wide constant in the memory;

using a portion of the cryptography key to DES-encrypt the system-wide constant, thereby producing a first key-check value generation result;

using a portion of the cryptography key to DES-decrypt the first key-check value generation result, thereby producing a second key-check value generation result;

using a portion of the cryptography key to DES-encrypt the second key-check value generation result, thereby producing a third key-check value generation result; and

selecting a portion of the third key-check value generation result for use as a key-check value.

49. (Twice previously amended) A method for generating identification data for a non-ATM electronic financial transaction over a communications network, comprising the steps of:

providing a first set of identification data related to a first transaction type;

performing a cryptographic operation upon the first set of identification data to generate a second set of identification data for use in conducting said non-ATM electronic financial transaction, wherein said first set of identification data is an ATM PIN, said first transaction type is an ATM-transaction, said second set of identification data is a non-ATM electronic commerce PIN; and

performing a second cryptographic operation upon said non-ATM electronic commerce PIN to generate said ATM PIN.

50. (Previously amended) The method of claim 49, further comprising the step of:

performing a second cryptographic operation upon said electronic commerce PIN to generate said ATM-PIN.